

1 CLAIMS

2

3 1. One or more computer-readable media having stored thereon a

4 plurality of instructions for generating a product identifier, wherein the plurality of

5 instructions, when executed by one or more processors, causes the one or more

6 processors to perform the following acts:

7 receiving a value;

8 padding the received value using a recognizable pattern;

9 converting the padded value to a number represented by a particular

10 number of bits;

11 converting the number to an element of the Jacobian of a curve;

12 raising the element to a particular power;

13 compressing the result of raising the element to the particular power; and

14 outputting, as the product identifier, the compressed result.

15

16 2. One or more computer-readable media as recited in claim 1, wherein

17 the receiving comprises receiving a numeric value associated with a copy of a

18 product.

19

20 3. One or more computer-readable media as recited in claim 1, wherein

21 the recognizable pattern comprises at least a portion of the received value.

22

23

24

25

1           4.     One or more computer-readable media as recited in claim 1, wherein  
2 converting the padded value to a number represented by a particular number of  
3 bits comprises converting the padded value to a 114-bit number.

4  
5           5.     One or more computer-readable media as recited in claim 1, wherein  
6 converting the padded value to a number represented by a particular number of  
7 bits comprises:

8                 defining a plurality of functions, wherein each of the plurality of functions  
9 returns a value that is a set of bits of a hash value generated based on an input  
10 value;

11                 separating the padded value into a plurality of portions; and

12                 using the plurality of portions as input values for the plurality of functions.

13  
14           6.     One or more computer-readable media as recited in claim 5, wherein  
15 each of the plurality of functions returns a set of least significant bits of a hash  
16 value generated based on the input.

17  
18           7.     One or more computer-readable media as recited in claim 5, wherein  
19 the hash value is generated using a secure hashing process.

20  
21           8.     One or more computer-readable media as recited in claim 5, wherein  
22 the set of bits includes a number of bits equal to half the particular number of bits.  
23  
24  
25

1           9.     One or more computer-readable media as recited in claim 5, wherein  
2 the separating comprises separating the padded value into two equal portions.

3  
4           10.    One or more computer-readable media as recited in claim 1, wherein  
5 the curve comprises a hyperelliptic curve.

6  
7           11.    One or more computer-readable media as recited in claim 1, wherein  
8 converting the number to an element of the Jacobian of the curve is based at least  
9 in part on an order of a group of points on the Jacobian of the curve, and wherein  
10 the order of the group of points on the Jacobian of the curve is maintained as a  
11 secret.

12  
13          12.    One or more computer-readable media as recited in claim 1, wherein  
14 the curve is given by the equation  $y^2=f(x)$ , wherein  $f(x)$  has a degree of  $2 \cdot g + 1$ , and  
15 wherein  $g$  refers to the genus of the curve.

16  
17          13.    One or more computer-readable media as recited in claim 12,  
18 wherein converting the number to an element of the Jacobian of a curve  
19 comprises:

20           determining a value  $a(x)$ , wherein the value  $a(x)$  is a monic irreducible  
21 polynomial of degree  $g$ ;

22           determining a value  $b(x)$ , wherein the value  $b(x)$  is a square root of  $f(x)$   
23 modulo  $a(x)$  of degree less than  $a(x)$ ; and

24           using, as the element of the Jacobian of the curve, the values  $a(x)$  and  $b(x)$ .  
25

1           **14.** One or more computer-readable media having stored thereon a  
2 plurality of instructions that, when executed by one or more processors, causes the  
3 one or more processors to perform the following acts:

4           receiving a product identifier;

5           decompressing the product identifier to obtain a decompressed value;

6           raising the decompressed value to a particular exponent to obtain a  
7 resulting value, wherein the raising is based at least in part on an element of a  
8 Jacobian of a curve;

9           converting the resulting value to a number having a particular number of  
10 bits;

11           checking whether a set of bits of the particular number of bits represents a  
12 recognizable pattern; and

13           determining that the product identifier is valid if the set of bits do represent  
14 the recognizable pattern, and otherwise determining that the product identifier is  
15 invalid.

16  
17           **15.** One or more computer-readable media as recited in claim 14,  
18 wherein the recognizable pattern comprises a duplicate of at least a portion of part  
19 of the resulting value.

20  
21           **16.** One or more computer-readable media as recited in claim 14,  
22 wherein the curve comprises a hyperelliptic curve.  
23  
24  
25

1           17. One or more computer-readable media as recited in claim 14,  
2 wherein the raising is further based at least in part on an order of a group of points  
3 on the Jacobian of the curve, and wherein the order of the group of points on the  
4 Jacobian of the curve is maintained as a secret.

5  
6           18. One or more computer-readable media as recited in claim 14,  
7 allowing a software product associated with the product identifier to be installed  
8 only if the product identifier is determined to be valid.

9  
10          19. One or more computer-readable media as recited in claim 14,  
11 wherein the plurality of instructions further causes the one or more processors to  
12 perform the following acts:

13           recovering another set of bits from the particular number of bits;

14           checking whether the other set of bits corresponds to a particular product;

15           and

16           determining that authentication of the particular product succeeds if the  
17 other set of bits corresponds to the particular product, and otherwise determining  
18 that authentication of the particular product fails.

19  
20          20. A method comprising:

21           receiving an encrypted product identifier;

22           recovering a plaintext message from the encrypted product identifier,

23 wherein the recovering is based on a secret that is the size of a group of points on a  
24 Jacobian of a curve;

25           checking whether the plaintext message includes a particular value; and

1 determining that the encrypted product identifier is valid if the plaintext  
2 message includes the particular value, and otherwise determining that the  
3 encrypted product identifier is invalid.  
4

5 **21.** A method as recited in claim 20, wherein the particular value  
6 comprises a duplicate of at least a portion of part of the plaintext message.  
7

8 **22.** A method as recited in claim 20, wherein the curve comprises a  
9 hyperelliptic curve.  
10

11 **23.** A method as recited in claim 20, wherein the recovering comprises:  
12 decompressing the encrypted product identifier to obtain a decompressed  
13 value;  
14

15 raising the decompressed value to a particular exponent to obtain a  
16 resulting value, wherein the raising is based at least in part on the size of the group  
17 of points on the Jacobian of the curve; and  
18

19 converting the resulting value to a number having a particular number of  
20 bits, wherein the number comprises the plaintext message.  
21

22 **24.** A method as recited in claim 20, wherein the particular value  
23 comprises a particular pattern.  
24  
25

1           **25.**    A method as recited in claim 20, further comprising:  
2           allowing a software product associated with the encrypted product  
3 identifier to be installed only if the encrypted product identifier is determined to be  
4 valid.

5  
6           **26.**    A method as recited in claim 20, further comprising:  
7           checking a numeric value embedded in the plaintext message; and  
8           determining, based on the numeric value, whether the encrypted product  
9 identifier corresponds to an authentic copy of a product

10  
11           **27.**    A method as recited in claim 20, further comprising:  
12           comparing the numeric value to a record of numeric values; and  
13           determining that the encrypted product identifier corresponds to an  
14 authentic copy of the product if the number value is included in the record of  
15 number values, and otherwise determining that the encrypted product identifier  
16 does not correspond to an authentic copy of the product.

17  
18           **28.**    An encryption method, comprising:  
19           encrypting a message using a secret; and  
20           wherein the secret comprises the order of a group of points on the Jacobian.

21  
22           **29.**    An encryption method as recited in claim 28, wherein the encrypting  
23 comprises:  
24           receiving the message;  
25           padding the received message using a recognizable pattern;

1 converting the padded message to a number represented by a particular  
2 number of bits;

3 converting the number to an element of the Jacobian of a curve;

4 raising the element to a particular power;

5 compressing the result of raising the element to the particular power; and

6 outputting, as an encrypted message, the compressed result.

7  
8 **30.** An encryption method as recited in claim 28, wherein the Jacobian  
9 comprises a Jacobian of a hyperelliptic curve.

10  
11 **31.** An encryption method as recited in claim 28, wherein the secret  
12 comprises the order of a group of points on the Jacobian of a curve, wherein the  
13 curve is given by the equation  $y^2=f(x)$ , wherein  $f(x)$  has a degree of  $2\cdot g+1$ , and  
14 wherein  $g$  refers to the genus of the curve.

15  
16 **32.** An encryption method as recited in claim 28, wherein the message  
17 comprises a numeric value corresponding to a copy of a product, and wherein the  
18 encrypting creates a ciphertext that is a product identifier corresponding to the  
19 copy of the product.

20  
21 **33.** An encryption method as recited in claim 32, wherein the numeric  
22 value corresponds to only one copy of the product.

23  
24 **34.** A decryption method, comprising:

25 decrypting a message using a secret; and



1 wherein the secret comprises the order of a group of points on a Jacobian of  
2 a curve.

3  
4 **35.** A decryption method as recited in claim 34, wherein the curve  
5 comprises a hyperelliptic curve.

6  
7 **36.** A decryption method as recited in claim 34, further comprising:  
8 recovering a portion of the decrypted message;  
9 checking whether the portion of the decrypted message corresponds to a  
10 particular product; and

11 determining that authentication of the particular product succeeds if the  
12 portion of the decrypted message corresponds to the particular product, and  
13 otherwise determining that authentication of the particular product fails.

14  
15 **37.** A decryption method as recited in claim 34, wherein the message  
16 comprises a product identifier corresponding to a copy of a product.

17  
18 **38.** A decryption method as recited in claim 34, wherein decrypting the  
19 message comprises:

20 decompressing the message to obtain a decompressed value;

21 raising the decompressed value to a particular exponent to obtain a  
22 resulting value, wherein the raising is based at least in part on the order of the  
23 group of points on the Jacobian of the curve; and

24 converting the resulting value to a number having a particular number of  
25 bits.

1  
2       **39.**     A decryption method as recited in claim 38, further comprising:  
3       checking whether a set of bits of the particular number of bits represents a  
4 recognizable pattern; and  
5       determining that the product identifier is valid if the set of bits do represent  
6 the recognizable pattern, and otherwise determining that the product identifier is  
7 invalid.

8  
9       **40.**     A system comprising:  
10      an input module to receive a plaintext message to be encrypted; and  
11      an encryption module, communicatively coupled to the input module, to  
12 convert the plaintext message to ciphertext based on both a curve and a group of  
13 points on a Jacobian of the curve.

14  
15      **41.**     A system as recited in claim 40, wherein the system further  
16 comprises:  
17      a curve selection module, communicatively coupled to the encryption  
18 module, configured to select the curve and the Jacobian of the curve base at least  
19 in part on a set of input parameters.

20  
21      **42.**     A system as recited in claim 41, wherein the input parameters  
22 include both a genus of the curve and the order of a Jacobian of the curve.  
23  
24  
25

1           **43.**    A system as recited in claim 40, wherein the curve comprises a  
2 hyperelliptic curve.

3  
4           **44.**    A system as recited in claim 40, wherein the encryption module is  
5 configured to convert the plaintext message to ciphertext by:

6               padding the plaintext message using a recognizable pattern;

7               converting the padded message to a number represented by a particular  
8 number of bits;

9               converting the number to an element of the Jacobian of the curve, wherein  
10 the converting is based at least in part on the group of points on the Jacobian of the  
11 curve;

12              raising the element to a particular power; and

13              outputting, as the ciphertext, the result of raising the element to the  
14 particular power.

15  
16           **45.**    A system comprising:

17               an input module to receive a ciphertext; and

18               a decryption module, communicatively coupled to the input module, to  
19 convert the ciphertext to a plaintext message based on both a curve and a group of  
20 points on a Jacobian of the curve.

21  
22           **46.**    A system as recited in claim 45, wherein the curve comprises a  
23 hyperelliptic curve.

1        47.    A system as recited in claim 45, wherein the decryption module is  
2 configured to convert the ciphertext to a plaintext message by:

3        decompressing the ciphertext to obtain a decompressed value;

4        raising the decompressed value to a particular exponent to obtain a  
5 resulting value, wherein the raising is based at least in part on the order of the  
6 group of points on the Jacobian of the curve;

7        converting the resulting value to a number having a particular number of  
8 bits;

9        selecting a portion of the resulting value; and

10       using, as the plaintext message, the selected portion of the resulting value.  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25